



BLINK[®] Professional Endpoint Protection Platform



While signature-based anti-virus continues to be the primary endpoint protection mechanism in use today, there is a major shift occurring towards integrated threat management to enhance security. Desktop administrators are constantly struggling to prevent attacks against unpatched endpoints and are tired of installing new agents each time a spyware, phishing attack, remote exploit, or other new threat is identified. Using standalone anti-virus is a tactical approach that drains system resources, depletes IT budgets and fails to prevent zero-day attacks.

Complicating the endpoint security equation further is the breakdown of client-server network architectures. As mainstream adoption of virtualization, mobile, wireless and remote access technologies force the traditional network perimeter to dissolve, the opportunity for worms and viruses to propagate has increased dramatically. In response, perimeter and network security capabilities are increasingly required on host endpoints.

Fast Facts

o Blink Provides Complete Endpoint Protection Security by Combining:

- Application and system firewall
- Virus and spyware protection
- Protocol-based intrusion prevention
- Vulnerability assessment
- Patented system protection
- Zero-day attack protection
- Dynamic policy support

Integrated Threat Management: Complete Endpoint Protection

To enhance endpoint security and combat threats in real-time, organizations are migrating off of standalone anti-virus and adopting integrated threat management instead. Blink 4, from eEye Digital Security, combines multiple-layers of endpoint security capabilities and leverages a host-based intrusion prevention engine that dynamically collects and incorporates new threat data in real-time. Since the product was launched in 2006, it has successfully thwarted 100% of remote intrusion attempts. Blink 4 provides a complete endpoint protection platform with full-featured integrated threat management capabilities. Blink 4 delivers a host of positive business benefits:

- Layered security protection that optimizes defenses against viruses, spyware, worms, Trojans, and other malicious zero-day exploits
- The ability to consolidate 5+ discrete endpoint security agents into 1 Blink 4 agent and reap significant administrative time savings in the process
- Reduce system resource requirements by over 50% compared to the memory footprint of maintaining 5+ discrete endpoint security products
- Reduce endpoint security costs by over 50% by eliminating the licensing and support costs associated with buying and maintaining multiple endpoint security products
- Gain centralized policy control over applications, system resources, and removable storage devices
- Combine Blink 4 with REM, eEye's Security Management Console, to obtain centralized attack, risk, vulnerability and overall security management

Please visit www.eEye.com to request an evaluation copy of Blink Professional 4 or to download a free copy of Blink Personal and find out for yourself why Blink garners the highest praise in independent product reviews.

"eEye performed best in detecting exploits. It was the clear leader in identifying client-side attacks, alerting on all of our tests."

- Information Security Magazine, November 2007

**Secure
Your Business.**
www.eEye.com
866-282-8276

The endpoint to vulnerability starts here.

BLINK® Professional

Additional Features and Benefits

- Firewall Protection

Blink performs traditional firewall duties, allowing or denying traffic based on a set of predetermined rules. Blink also monitors the source of network traffic in real time and only allows traffic from authorized applications, preventing unauthorized programs from making illegal outbound connections.

- Virus and Spyware Protection

Blink provides complete signature and heuristics-based attack protection. Using patented sandbox technology, Blink actively blocks malicious activity from being loaded into memory. Signatures provide an additional protection layer but Blink is not signature dependent and can stop new attacks as they are released without the need for updates.

- Intrusion Prevention

Blink provides protection where a vendor has not yet created signatures or patches to protect against vulnerabilities in their operating system or application. Blink blocks “zero-day” attacks that bypass traditional signature-based solutions, eliminating the need or use of specific attack signatures.

- System Protection

Blink provides control over which applications are allowed to function by authorizing or denying program file execution. Registry Protection prevents specific registry settings from being modified, stopping malicious programs from infecting or modifying systems. Storage Protection prevents data leakage by regulating USB and Firewire storage devices.

- REM® Security Management Console

Combined with REM, the integrated solution provides event and state analysis capabilities along with security and compliance reporting. The REM Security Management Console integrates attack-related information with local and network vulnerability assessment data, providing a complete security picture.

- ActiveX Protection

Blink ActiveX protection is based on Patent Pending technology that blocks threats at the lowest common denominator attack vector. This occurs by interfacing with the ActiveX system itself and using heuristics, signatures, and identification of suspicious calls, provides 100% effectiveness at blocking illegal remote code execution.

About eEye Digital Security

eEye Digital Security is the global leader in the next generation of security solutions: comprehensive vulnerability management and zero-day endpoint security protection.

eEye enables secure computing through world-renowned research and innovative technology, supplying the world's largest businesses with integrated and research-driven vulnerability assessment, intrusion prevention, asset security and compliance solutions. eEye's research team is consistently the first to identify new threats in the wild and our products leverage that research to deliver the tools necessary to protect our customers' environments. The endpoint to vulnerability starts here.

eEye's customers represent the largest deployments of vulnerability assessment and prevention technology in the private and public sectors. eEye protects the networks and digital assets of a growing network of more than 9,000 corporate and government deployments worldwide. Founded in 1998, eEye Digital Security is an award-winning CA internet security company headquartered in Orange County, California.

U.S. Tel: 1.866.282.8276

N. America: 1.949.333.1900

Germany: +49 (0) 8031 2227 432

U.K.: +44 (0) 20 8432 3490

N. America Sales: sales@eEye.com

International Sales: sales.eu@eEye.com



System Requirements

Blink® Professional Edition

- Windows 7 (32-bit or 64-bit)
- Windows Server 2008 R2 (64-bit)
- Windows 2000 Professional
- Windows 2000 Server
- Windows XP (32-bit and 64-bit)
- Windows Server 2003 (32-bit and 64-bit)
- Windows Vista SP1 (32-bit or 64-bit)
- Windows Server 2008 (32-bit or 64-bit)
- Intel Pentium III 800Mhz (or compatible)
- 512MB of RAM
- At least 80MB of free disk space
- Network Interface Card (NIC) with TCP/IP enabled

The endpoint to vulnerability starts here.